Remarks

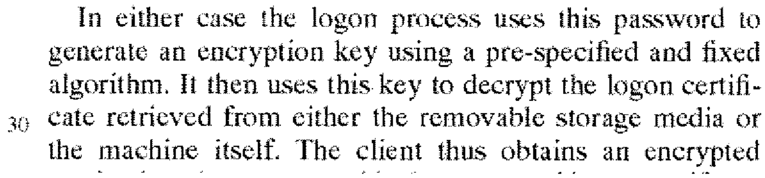
Claims 1-72 are pending in the application. Claims 1-72 are rejected. All rejections are respectfully traversed.

The invention re-authenticates and protects communication security. Using a key lease generated by performance of a primary authentication protocol, a secondary authentication protocol is performed between a client electronic system (client) and a network access point electronic system (AP). The key lease includes a key lease period for indicating a length of time in which the key lease is valid for using the secondary authentication protocol instead of the primary authentication protocol. If the secondary authentication protocol is successful, a session encryption key is generated for encrypting communication traffic between said client and said AP.

Claims 1, 12, 23, 34-36, 47-49, and 60-62 are rejected under 35 U.S.C. 102(b) as being anticipated by Misra, et al., (U.S. 5,999,711 – Misra).

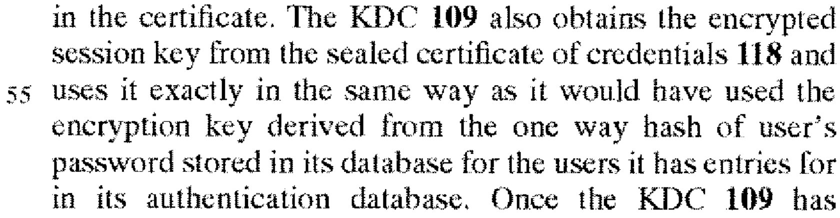
Misra describes a method for authentication and authorization to allow a user to logon to a distributed system outside of a home domain of the user. Misra describes generating a certificate including both authentication information and authorization rights. In contrast, the invention re-authenticates a client electronic system using a secondary authentication protocol. Authorization would never be confused with authentication or re-authentication by a person of ordinary skill in the art.

Claimed is performing a secondary authentication protocol between a client electronic system (client) and a network access point electronic system (AP) using a key lease generated by performance of a primary authentication protocol. At col. 8, lines 38-65, Misra describes only one authentication protocol, which is used for either a user logging into his own domain, or another domain on the4 distributed system, see e.g., col. 8, lines 27-29, below:



In either case the logon process uses this password to generate an encryption key using a pre-specified and fixed algorithm. It then uses this key to decrypt the logon certificate retrieved from either the removable storage media or the machine itself. The client thus obtains an encrypted

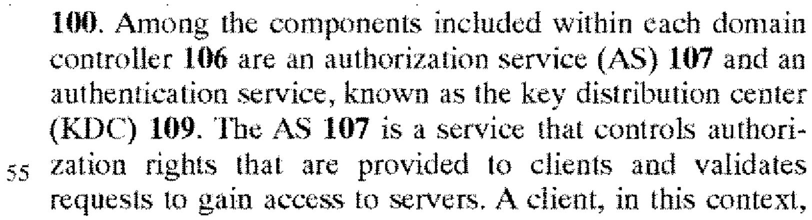
See also, col. 8, lines 53-58, below:



in the certificate. The KDC **109** also obtains the encrypted session key from the sealed certificate of credentials **118** and uses it exactly in the same way as it would have used the encryption key derived from the one way hash of user's password stored in its database for the users it has entries for in its authentication database. Once the KDC **109** has

It appears that the Examiner mistakenly believes that Misra teaches two protocols for authentication simply because the KDC obtains an encrypted session key from the sealed certificate of credentials, see col. 8, line 53. However, that has nothing to do with primary or secondary authentication protocols. There is only one authentication protocol described in Misra. Misra never re-authenticates anything using a secondary authentication protocol, as claimed. The Examiner is requested to point out exactly which words mean primary authentication protocol and which words mean secondary authentication protocol in col. 8, lines 38-65 of Misra. The Applicants assert that Misra never describes re-authentication using a secondary authentication protocol, as claimed.

Further Misra at col. 8, line 66 – col. 9, line 43 describes authorization, not authentication. As stated above, a person of ordinary skill in the art would never confuse authorization would never be confused with authentication or re-authentication, as claimed. Misra even points out the distinction at col. 4, lines 51-56, below:



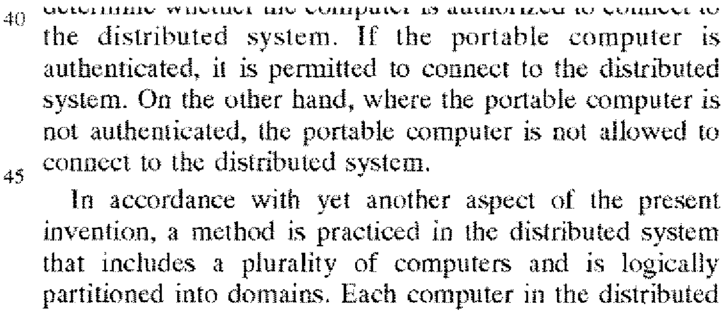
100. Among the components included within each domain controller **106** are an authorization service (AS) **107** and an authentication service, known as the key distribution center (KDC) **109**. The AS **107** is a service that controls authorization rights that are provided to clients and validates requests to gain access to servers. A client, in this context,

The authorization described in Misra can never anticipate what is claimed. Therefore, for at least the reasons stated above, the Examiner is requested to reconsider and withdraw the rejection of claims 1, 12, 23, 34-36, 47-49, and 60-62 based on Misra.

Regarding claims 34, 47, and 60, the Examiner points to col8, line 66- col. 9, line 43, which, as stated above, describes authorization services, not re-authentication using a secondary authentication protocol, as claimed. The same is true for claims 35-36, 48-49, and 61-62.

Claims 2-6, 13-17, and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra in view of Dole (U.S. 6,628,786).

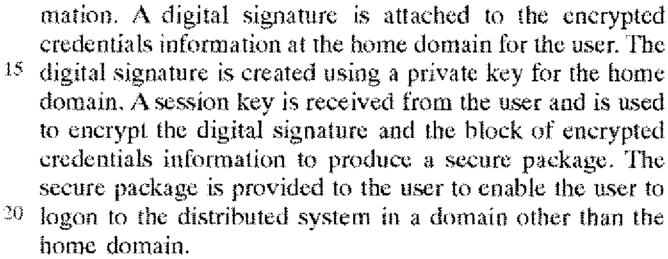
Claimed is transmitting the key lease generated using the first authentication protocol from said client to said AP. The key lease includes an encryption key for use in said secondary authentication protocol. The invention uses the primary protocol to authenticate the client and AP and the secondary protocol to re-authenticate. At column 2, lines 42-48, Misra states an unauthenticated is not allowed to connect to the distributed system, see lines 42-48, below:



determine whether the computer is authorized to connect to the distributed system. If the portable computer is authenticated, it is permitted to connect to the distributed system. On the other hand, where the portable computer is not authenticated, the portable computer is not allowed to connect to the distributed system.

In accordance with yet another aspect of the present invention, a method is practiced in the distributed system that includes a plurality of computers and is logically partitioned into domains. Each computer in the distributed

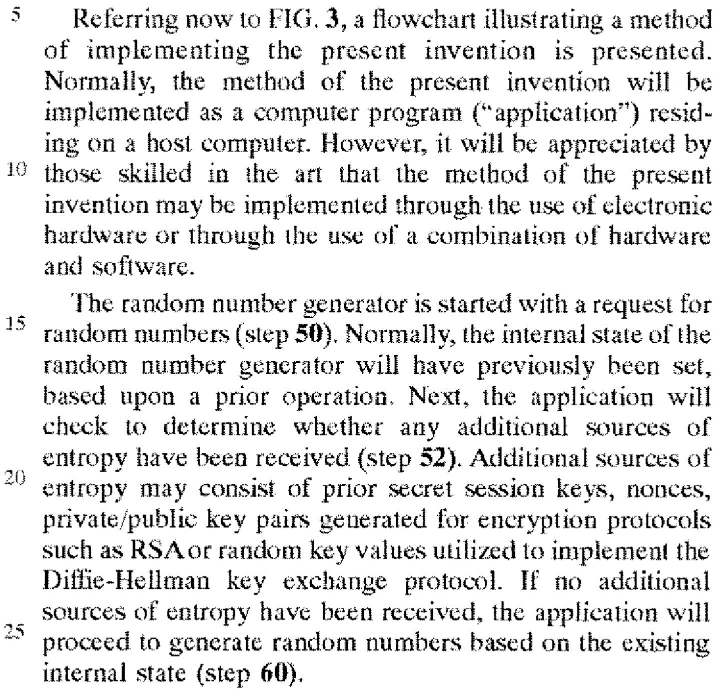
The Examiner is requested to explain exactly how the above teaches transmitting the key lease from the client to the AP," as claimed. Further, the Examiner is requested to explain how lines 13-21 teach "the key lease includes an encryption key for use in said secondary authentication protocol," as claimed. See lines 13-21, below:



mation. A digital signature is attached to the encrypted credentials information at the home domain for the user. The digital signature is created using a private key for the home domain. A session key is received from the user and is used to encrypt the digital signature and the block of encrypted credentials information to produce a secure package. The secure package is provided to the user to enable the user to logon to the distributed system in a domain other than the home domain.

A person of ordinary skill in the art would readily understand after carefully reading Misra that the above describes the authentication and authorization method, not authentication and re-authentication, as claimed. Misra fails to teach authentication using a primary protocol, and then re-authentication using a secondary protocol and a key lease generated by performance of the primary authentication protocol, as claimed. Dole fails to cure the defects of Misra.

Dole describes a random number generation method used for encrypting communications between computers. The Examiner's assertion that Dole teaches generating a first random number associated with said client and a second random number associated with said AP as claimed, is pure conjecture because there is never any description of associating random numbers with a computer such as a client or AP in col. 6, lines 5-27, see below:



Referring now to FIG. **3**, a flowchart illustrating a method of implementing the present invention is presented. Normally, the method of the present invention will be implemented as a computer program ("application") residing on a host computer. However, it will be appreciated by those skilled in the art that the method of the present invention may be implemented through the use of electronic hardware or through the use of a combination of hardware and software.

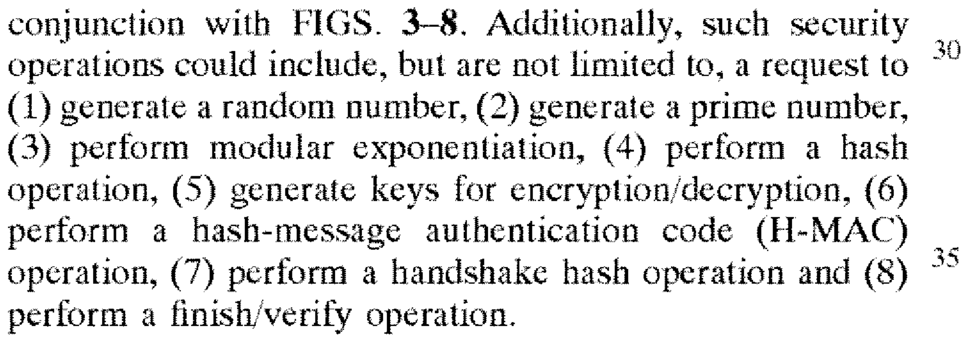
The random number generator is started with a request for random numbers (step **50**). Normally, the internal state of the random number generator will have previously been set, based upon a prior operation. Next, the application will check to determine whether any additional sources of entropy have been received (step **52**). Additional sources of entropy may consist of prior secret session keys, nonces, private/public key pairs generated for encryption protocols such as RSA or random key values utilized to implement the Diffie-Hellman key exchange protocol. If no additional sources of entropy have been received, the application will proceed to generate random numbers based on the existing internal state (step **60**).

The Examiner is requested to specifically point out exactly which words above mean generating a first random number associated with said client and a second random number associated with said AP, as claimed. The applicants see only random number generation for encryption purposes. Further still, there is no teaching of a secondary authentication protocol, or re-authenticating.

The hashing described in Dole is for encryption of a particular message and has nothing to do with a secondary authentication protocol using a key lease from performance of a primary authentication protocol, as claimed. Regarding claims 6, 17 and 28, Misra never describes a secondary authentication protocol, as claimed. Therefore, the keys described by Misra are irrelevant to what is claimed.

Claims 7-11, 18-22, and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra in view of Dole and in further view of Kessler, et al., (U.S. 6,789,147 – Kessler).

Claimed is using said encryption key, said first random number, said second random number, a first media access control (MAC) address associated with said client, a second media access control (MAC) address associated with said AP, and a hash function to determine said first and second session encryption keys. The section at col. 5, lines 18-27 referenced by the Examiner does not even hint at generating first and second session encryption keys based on the explicitly recited elements above, see, e.g., col. 5, lines 29-32, below:



conjunction with FIGS. **3–8**. Additionally, such security operations could include, but are not limited to, a request to (1) generate a random number, (2) generate a prime number, (3) perform modular exponentiation, (4) perform a hash operation, (5) generate keys for encryption/decryption, (6) perform a hash-message authentication code (H-MAC) operation, (7) perform a handshake hash operation and (8) perform a finish/verify operation.

There is nothing above that describes the explicitly claimed combination of elements to generate the first and second session keys, as claimed.

The same is true for the claimed applying a HMAC-MDS algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key. There is no description of applying HMAC-MDS algorithm to the particular concatenation to produce either a first or second session key as recited in the claims. The Examiner is also reminded that the invention re-authenticates using a second authentication protocol and a key lease from a primary authentication protocol. No such thing is ever considered by Misra, Dole, or Kessler.

Claims 37, 50, and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra in view of Kennelly et al., (U.S. 6,754,702 – Kennelly).

As stated above with respect to claim 34, Misra fails to teach authenticating using a primary authentication protocol and re-authenticating using a secondary authentication protocol, as claimed. Kennelly fails to cure that defect. Further, Kennelly applies user attribute information to determine authorization levels during a session. This has nothing to do with the claimed authentication. The invention uses context information to determine a length of tie a key lease is valid during the secondary authentication protocol. Kennally is useless for making the invention obvious.

Claims 38-43, 51-56, and 64-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra in view of Babu, et al., (U.S. 6,122,639 – Babu).

As stated above, Misra fails to teach primary and secondary authentication protocols for authenticating and re-authenticating, as claimed. The Examiner's assertions that Misra teaches a key lease from performing a primary authentication protocol includes identifiers for secondary authentication protocols is simply erroneous, as discussed above.

Babu describes a change detection application used for network management in a manage information base (MIB) and is completely outside of the field of endeavor of the invention and Misra. Babu has nothing to do with either Misra or what is claimed. There is no motivation to combine those refernces, nor would a combination be operable for either intended purpose.

Claims 44, 57, and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra in view of Kung, et al., (U.S. 5,434,918 – Kung).

Claimed is wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on symmetric encryption. As stated above, Misra fails to teach authentication and re-authentication using primary and secondary authentication protocols, as claimed.

Kung describes a mutual authentication protocol using random numbers, user IDs and passwords to complete the mutual authentication. Kung only authenticates (mutually) using a single authentication protocol. Kung never describes authentication and re-authentication using primary and secondary authentication protocols, as claimed. Therefore, Kung fails to cure the defects of Misra an cannot be used to make the invention obvious.

Claims 45, 58, and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Misra in view of Burns, et al., (U.S. 6,792,424 – Burns).

Claimed is wherein said secondary authentication protocol comprises a mutual challenge-response protocol based on a one-way hash function message authentication code (HMAC) implementation. As stated above, Misra fails to teach authentication and re-authentication using primary and secondary authentication protocols, as claimed.

Burns describes a method that authenticates and then provides authorization based on a color classification system. Again, a person of ordinary skill in the art would never confuse authentication with authorization. Burns never describes authentication and re-authentication using primary and secondary authentication protocols, as claimed. Therefore, Burns fails to cure the defects of Misra an cannot be used to make the invention obvious.

The same is true for claims 46, 59, and 72.

It is believed that this application is now in condition for allowance. A notice to this effect is respectfully requested. Should further questions arise concerning this application, the Examiner is invited to call Applicant's attorney at the number listed below.

Please charge any shortage in fees due in connection with the filing of this paper to Deposit Account 50-3650.

Respectfully submitted,
3Com Corporation,

By

Andrew J. Curtin
Attorney for the Assignee
Reg. No. 48,485

350 Campus Drive
Marlborough, MA 01752
Telephone: (508) 323-1330
Customer No. 56436